

**BY ORDER OF THE COMMANDER  
AIR FORCE WEATHER AGENCY**



**AIR FORCE WEATHER AGENCY  
HEADQUARTERS OPERATING  
INSTRUCTION 33-19**

**10 AUGUST 2005**

**Communications and Information  
SECURE TELEPHONE PROGRAM**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>.

---

OPR: HQ AFWA/XOGR  
(Mr. Michael T. Kochaver)  
Supersedes AFWAHOI33-19, 30 September 1999

Certified by: HQ AFWA/XOG  
(Lt Col Rod Clements)  
Pages: 5  
Distribution: F

---

This Headquarters Operating Instruction (HOI) defines security responsibilities and procedures for Headquarters Air Force Weather Agency (HQ AFWA) personnel operating Secure Terminal Equipment (STE) and Secure Telephone Unit (STU-III) telephone systems and implements

Air Force Instruction 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type 1*. It provides specific guidance on the operation and protection of STE/STU-III telephones and associated KOV-14 Cards (used with STEs) and Crypto Ignition Keys (CIK), used with STU-IIIIs. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual 37-123, *Management of Records*, and disposed of IAW Air Force Web RIMS Records Disposition Schedule located at <https://webrims.amc.af.mil/rds/index.cfm>.

**SUMMARY OF REVISIONS**

Updates instruction to account for transition from STU-III to STE telephone systems.

**1. Applicability.** The STE and STU-III are user-friendly telephone desk sets that provide secure voice and data capability. The STE and STU-III/Low Cost Terminal (LCT) can operate in a secure or nonsecure mode at the simple push of a button. They provide a low maintenance, simple to operate and maintain, secure voice/data instrument. STU-III telephones will not be able to operate without additional pieces of equipment in FY2007 and should be replaced with STE's as soon as possible.

**2. Duties and Responsibilities.**

**2.1. Secure Telephone Monitors and Alternates.**

2.1.1. Provide guidance to HQ AFWA STE and STU-III users as needed.

2.1.2. Order KOV-14 cards for STE systems and CIKs for all HQ AFWA STU-III systems as needed. Conduct or oversee keying process for each system. Return Form L3794, **Crypto Ignition Key Log**, to 55 CS/SCBSC, COMSEC Flight, as soon as possible after keying a system. Also, return any keys not needed or zeroized.

2.1.3. Order Network Encryption System (NES) keys as needed.

2.1.4. Ensure unkeyed KOV-14 cards and CIKs in unopened plastic pink containers are accounted for using AFCOMSEC Form 16, **COMSEC Account Daily Shift Inventory**. These unkeyed Cards/CIKs must be stored in an approved General Services Administration (GSA) security container and should be keyed to the appropriate terminal as soon as possible. Accountability terminates after the Card/CIK is keyed.

2.1.5. Prepare and submit to 55 CS/SCBSC, COMSEC Flight, a STE/STU-III Key Management Report at least annually or when significant changes occur. This report identifies all HQ AFWA STE/STU-III systems, location, and Card/CIK serial numbers.

2.1.6. Conduct or oversee quarterly rekeying of all HQ AFWA STE/STU-III systems. Rekeying is done by calling the Key Management Center at DSN 936-1810. The card/key must be in the phone when re-keying.

2.1.7. Update appointment memorandums at least annually or when there is a change. Provide the appointment memorandum to the AFWA CRO.

2.1.8. Attend 55 CS/SCB, Information Systems Flight, STU-III training class at least annually.

2.1.9. Review this HOI at least annually to ensure currency.

### 3. Procedures.

#### 3.1. Making a Secure Call.

3.1.1. Ensure uncleared/unauthorized personnel are not in the area, and restrict access until the classified telephone call is terminated.

3.1.2. Establish a nonsecure call to the desired party and announce your intentions to go secure (they must also be on a STE or STU-III).

3.1.3. Insert the KOV-14 card or CIK and turn it clockwise.

3.1.4. Tell them you are “Going to Go Secure” and press the SECURE (voice) button. The distant end may initiate going secure by pressing the SECURE button at their terminal; however, only one person should press the SECURE button. DO NOT discuss classified information until the secure mode is established.

3.1.5. The information in the display window will confirm the terminal is in a secure mode and what classification level you can discuss. The classification is determined by the highest mutual level, i.e., if one is TOP SECRET and the other is SECRET then the highest mutual level is SECRET.

3.1.5.1. The terminal window displays administrative information of the distant terminal.

3.1.5.2. The information displayed does not necessarily authenticate the person using the distant end STE/STU-III. Therefore, users must use judgment in determining the

“need-to-know.” Use the terminal window display to the fullest extent to ensure STE/STU-III terminal system integrity.

3.1.6. When operationally required, authorized persons may permit others not normally authorized to use the keyed terminal under the following conditions:

3.1.6.1. An authorized person must place the call.

3.1.6.2. After reaching the called party, the caller will identify the individual on whose behalf the call is being made and their clearance level.

3.1.7. When you are finished talking secure, depress the ‘NONSECURE’ (voice) button (alternatively, the distant end may initiate going nonsecure by pressing NONSECURE at their terminal). To confirm NONSECURE, ensure the display window states “NONSECURE.”

3.1.8. Hang up the phone when the terminal has returned to the NONSECURE mode. **Never hang up the phone while the terminal is in the secure mode or the key may become zeroized.**

3.1.9. The card/key may be left in the STE/STU-III if it’s located in a classified work area that is manned 24-hours per day. In the event of a full evacuation of the area where the STE/STU-III is located, the card/CIK must be removed from the system and secured in a safe or be carried out of the area and replaced when the individual returns.

### 3.2. Use of STE/STU-III, Nonsecure Mode.

3.2.1. The STE/STU-III is considered an unclassified COMSEC Controlled Item (CCI) when unkeyed (when the KOV-14/CIK is not inserted in the terminal). The terminal may be used for unclassified calls in this mode.

3.2.2. To make a nonsecure phone call, use the terminal the same as a normal phone. To confirm nonsecure, ensure the display window states “NONSECURE.”

## 4. Terminal Protection.

### 4.1. Safeguarding.

4.1.1. The following are acceptable ways to store: when the KOV-14/CIK is stored in the same room as the STU-III, store the CIK in a GSA approved security container. Only authorized STE/STU-III users may have access to the container. Another option is to store the KOV-14/CIK in a locked cabinet or desk, but in a different room from where the STE/STU-III system is kept.

4.1.2. The STE/STU-III terminal is considered an unclassified CCI when it is unkeyed. As a CCI item, you must protect the terminal as a high value item such as an electric typewriter or computer. Each STE/STU-III terminal is accountable through the equipment custodian. All personnel are responsible for the proper use and control of the terminal.

4.1.3. Use Standard Form 701, **Activity Security Checklist**, to conduct end-of-day security checks of STE/STU-III systems. The purpose of this check is to ensure the KOV-14/CIK has been removed by physically sighting the system. Indicate the serial number of the STE/STU-III systems being checked.

**5. Security Incidents.** Incidents on the STE/STU-III are somewhat unique. Only the user's prompt detection and reporting can minimize the compromise risk to the organization. If you feel you have an incident, immediately notify the HQ AFWA COMSEC Responsible Officer at DSN 272-9898.

**5.1. The Following are Incidents Unique to the STE/STU-III System:**

- 5.1.1. Any instance where the authentication information displayed during a secure call is not representative of the distant terminal.
- 5.1.2. Failure to adequately protect or to erase a KOV-14 or CIK associated with a lost terminal.
- 5.1.3. Any instance where the display indicates the distant terminal contains a compromised key.
- 5.1.4. Any lost or missing STE/STU-III terminals.
- 5.1.5. Leaving a KOV-14/CIK in or near a terminal when the terminal is not under the operational control and within view of at least one authorized appropriately cleared user.

**6. Forms Adopted.** Standard Form 701, **Activity Security Checklist**, AFCOMSEC Form 16, **COM-SEC Account Daily Shift Inventory**, Form L3794, **Crypto Ignition Key Log**.

JOHN M. LANICCI, Colonel, USAF  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

- AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type I*  
AFSAL 4001A, *Air Force COMSEC Publication Controlled Cryptographic Items*  
AFMAN 37-123, *Management of Records*

***Abbreviations and Acronyms***

- 55 CS/SCB**—Information Systems Flight  
**55 CS/SCBSC**—COMSEC Flight  
**CCI**—COMSEC Controlled Item  
**CIK**—Crypto Ignition Key  
**COMSEC**—Communication Security  
**GSA**—General Services Administration  
**HOI**—Headquarters Operating Instruction  
**HQ AFWA**—Headquarters Air Force Weather Agency  
**KOV-14 Card**—Cryptographic Card for STE  
**LCT**—Low Cost Terminal  
**NES**—Network Encryption System  
**STE**—Secure Terminal Equipment  
**STU-III**—Secure Telephone Unit